

---

11/5/8 (Item 1 from file: 60)

DIALOG(R)File 60: ANTE: Abstracts in New Tech & Engineer

(c) 2009 CSA. All rights reserved.

0000497624 IP Accession No: 2008017229

**Advanced encryption standard (AES) hardware cryptographic engine**

Snell, Dorian L

, USA

**Publisher Url:** <http://patft.uspto.gov/netacgi/nph->

[Parser?Sect1=PTO2&Sect2=HITOFF&u=/netaht ml/PTO/search-](http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=/netaht ml/PTO/search-adv.htm&r=1&p=1&f=G&l=50&d=PTXT&S1=72 95671.PN.&OS=pn/7295671&RS=PN/7295671)

[adv.htm&r=1&p=1&f=G&l=50&d=PTXT&S1=72 95671.PN.&OS=pn/7295671&](http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=/netaht ml/PTO/search-adv.htm&r=1&p=1&f=G&l=50&d=PTXT&S1=72 95671.PN.&OS=pn/7295671&RS=PN/7295671)

[RS=PN/7295671](http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=/netaht ml/PTO/search-adv.htm&r=1&p=1&f=G&l=50&d=PTXT&S1=72 95671.PN.&OS=pn/7295671&RS=PN/7295671)

**Document Type:** Patent

**Record Type:** Abstract

**Language:** English

**File Segment:** ANTE: Abstracts in New Technologies and Engineering

**Abstract:**

A cryptographic method and related implements the **Rijndael- AES** encryption standard. In one improvement, the decryption round keys are generated on a round by round basis from the final  $N_k$  round keys saved from a previous encryption key scheduling operation. Latency and memory requirements are thereby minimized. **S-boxes** for the **AES** key generation and cipher operation itself, may be implemented multiple times in different ways with different power signatures, with a pseudo-random selection of the pathway for the different bytes to be substituted. The premix operation occurs **simultaneously** with the generation of first round keys, and a dummy circuit with substantially identical timing as the real premix circuitry adds power consumption noise to the premix.

**Descriptors:** Keys; Encryption; Cryptography; Standards; Hardware; Power consumption; Circuits; Scheduling; Dummies; Time measurements; Noise; Engines; Pathways; Electric circuits